Introduktion

Kristoffer Kjærgaard Christensen
Temaredaktør

„Collect it all". Det var målsætningen for amerikanske NSA og deres samarbejdspartneres overvågning, hvis massive omfang for alvor blev bragt frem i offentlighedens søgelys af Edward Snowdens opsigtsvækkende afsløringer i sommeren 2013. Snowdens afsløringer blev således startskuddet for en offentlig debat om proportionerne af efterretningstjenesternes overvågning i forhold til hensynet til national sikkerhed og kampen mod terrorisme. Den ambitiøse målsætning vidner også om, at den teknologiske udvikling har haft store konsekvenser for efterretningstjenesternes overvågningspraksisser. Tidligere ville en så omfattende overvågning have været utænkelig, men digital overvågning og *big data* har i vores moderne, gennemdigitaliserede samfund medført nye muligheder i den henseende.

Vi lever i en tid, hvor digitale tjenester spiller en stadig større rolle i vores dagligdag. Vi kommunikerer via e-mails og sociale medier, tjekker nyheder og handler online, overfører penge via netbank, „googler" alt fra togtider til sygdomsdiagnoser, streamer musik og tv-serier, interagerer med det offentlige vha. NemID – for at blot nævne nogle få eksempler. Således efterlader vi alle sammen hver eneste dag – mere eller mindre frivilligt – en række digitale fodspor om alt mellem himmel og jord, og ved at tilgå og kombinere alle disse tidligere separate informationer kan man sammenstykke et sammenhængende billede af den enkeltes adfærd. Det skaber en masse nye muligheder for bl.a. skræddersyede ydelser og tjenester og er på mange måder med til at lette folks hverdag, men den stiller os også over for en række nye politiske dilemmaer og udfordringer. Registreringen af de store informationsmængder kombineret med de teknologiske muligheder for at tilgå og behandle dem udgør fx et enormt potentiale for efterretningstjenesterne, i og med at det muliggør en hidtil uset grad af overvågning af alle samfundets borgere.

De politiske dilemmaer og udfordringer i forbindelse med digital overvågning og brugen af *big data* gælder dog ikke kun spørgsmål om national sikkerhed og hemmelighedsfulde efterretningstjenester. Det vedrører i høj grad også private virksomheder. Hovedparten af de enorme datamængder genereres gennem privatejede tjenester, såsom fx Google, Facebook og Amazon. Detaljeret information om deres kunder er interessant for virksomhederne med henblik på fx at kortlægge forbrugernes adfærd og dermed målrette og forbedre deres produkter. Virksomhederne har altså en klar økonomisk interesse i disse data. Dermed bliver spørgsmålet om digital overvågning også spørgsmålet om, hvem der retmæssigt kan påberåbe sig rettighederne til data – den enkelte borger/bruger eller de private virksomheder – og til hvilke formål. Med andre ord: Må virksomhederne frit råde over deres viden om kunderne og anvende den til deres egne kommercielle formål? Den politiske og juridiske kamp om retten til virksomhedernes data om deres kunder er et tilbagevendende spørgsmål. Det blev bl.a. rejst i forbindelse med EU-Domstolens dom sidste år om retten til at få forkerte eller forældede oplysninger slettet fra Googles søgeresultater – også kendt som 'the right to be forgotten'.

Et andet vigtigt aspekt af private virksomheders håndtering af data omhandler ansvaret for at beskytte data. Hvilke forpligtelser har virksomhederne til at beskytte data mod hackerangreb, eller når statslige myndigheder kræver adgang til brugernes data? Et af de store stridspunkter i den seneste tid har fx været, hvorvidt virksomhederne bør inkorporere såkaldte '*backdoors*' – ved fx at opbevare krypteringsnøglerne (modsat såkaldt *end-to-end*-kryptering, hvor kun brugerne har krypteringsnøglerne) – så myndighederne kan få adgang til brugernes data, selv når de krypterede. Bl.a. Storbritanniens premierminister David Cameron og cheferne for henholdsvis FBI og NSA, James Comey og Michael Rogers, er blandt fortalerne for en sådan løsning, men de har dog mødt kraftig modstand blandt virksomhederne og andre, som ud over retten til privatliv har fremført, at eksistensen af *backdoors* vil gøre systemerne sårbare, i og med at terrorister og hackere også vil forsøge at skaffe sig adgang gennem de selvsamme *backdoors*. Spørgsmålet er desuden,

hvem der i sidste ende kan og skal træffe beslutningen om dette og lignende spørgsmål; hvilken lovgivning skal regulere håndteringen af data, når den som oftest foregår på tværs af grænser? Det dilemma afspejles blandt andet i den kontroversielle dom ved en amerikansk domstol, som forpligtede bl.a. Microsoft og Google til også at udlevere data om deres europæiske kunder til de amerikanske myndigheder, hvorimod 'the right to be forgotten' kun gælder for Google-søgninger foretaget i Europa.

Digital overvågning er således en vildtvoksende tematik, som gennemsyrer det moderne samfund – ikke blot som et spørgsmål om beskyttelse mod trusler mod den nationale sikkerhed, men som en væsentlig og integreret del af den enkeltes dagligdag. Det er ikke længere kontroversielt at sige, at vi lever i et overvågningssamfund, men det kan diskuteres, om det skal forstås i klassisk, Orwellsk og panoptisk forstand, eller om der er tale om en ny form for overvågning, og om denne udvikling er med til at påvirke vores forståelse af samfundet og de politiske og demokratiske principper og værdier, som samfundet hviler på. Udviklingen af digital overvågning kan opfattes som både konstruktiv og nødvendig og som problematisk og direkte farlig. Hvad vejer tungest; overvågningens betydning for efterretningstjenesternes arbejde for national sikkerhed, dens bidrag til funktionaliteten af de services, som faciliterer det moderne samfund, eller dens udfordring af borgernes privatliv? Sikkert er det, at digital overvågning rejser en lang række principielle, politiske og demokratiske spørgsmål angående forholdet mellem staten, borgerne og de private virksomheder, hensynet til statens sikkerhed, hensynet til borgernes ret til privatliv, behovet for gennemsigtighed og demokratisk kontrol, skellet mellem offentlig og privat med mere. Det er disse spørgsmål, som artiklerne i dette temanummer på forskellig vis forholder sig til.

Peter Lauritsen indleder temanummeret med at argumentere for at bruge begrebet 'den digitale dobbeltgænger' som udgangspunkt for at diskutere implikationerne af digital overvågning. Begrebet tager udgangspunkt i Haggerty & Ericsons analyse af *surveillant assemblages* og Latours oligoptikon-begreb. Herigennem ønsker Lauritsen at fremhæve overvågningens afgrænsethed, skrøbelighed og ikke mindst dens åbne indhold og formål. Lauritsen argumenterer for, at overvågning ikke nødvendigvis er totalitært og undertrykkende, men lige så vel kan være omsorgsfuldt, servicepræget og underholdende. Formålet med inddragelsen af digitale dobbeltgængere er således at flytte fokus fra overvågning som generelt fænomen til analyser af specifikke overvågningssituationer.

Karen Lund Petersen og Vibeke Schou Tjalve diskuterer, hvilke konsekvenser udviskningen af skellet mellem offentlig og privat som følge af introduktionen digital overvågning og *big data* har for bureaukratisk etik og demokratisk kontrol i forhold til efterretningstjenesternes virke i en tid, hvor sikkerhedspolitik i stigende grad drives af forestillingen om uforudsigelige risici. De argumenterer for vigtigheden af at forholde sig til etisk-demokratiske spørgsmål om ejerskab, ansvar og kontrol, når såvel statslige som civile aktører engageres i den sikkerhedspolitiske praksis og peger på, at efterretningstjenesternes øgede fokus på metode, regler og procedurer er forfejlet. I stedet argumenter de for en etisk tilgang med fokus på refleksiv og situationsbetinget dømmekraft.

Rikke Frank Jørgensen behandler i temaets tredje og sidste artikel spørgsmålet om rettigheden til privatliv. Retten til privatliv (*privacy*) anses for at være en menneskerettighed, men Jørgensen fremhæver, at denne rettighed er under pres fra såvel statslige myndigheder som private aktører i den digitale tidsalder, hvor skellet mellem det offentlige og private rum udfordres. I artiklen anviser hun tre potentielle løsningsmodeller: 1) Juridiske løsninger, 2) teknologiske løsninger (*privacy by design*) og 3) en grundlæggende gentænkning af online privatliv med fokus på konteksten, hvor data indsamles. Jørgensen argumenterer dog for, at hvis retten til privatliv skal overleve er det nødvendigt at sætte ind på alle tre områder.

Uden for tema bringer tidsskriftet i dette nummer Christian Rostbølls tiltrædelsesforelæsning i forbindelse med hans tiltræden som professor (mso) ved Institut for Statskundskab, Københavns Universitet. I forelæsningen forholder Rostbøll sig til kompromisets demokratiske betydning. Han argumenterer for kompromiset som et demokratisk ideal, der indebærer respekt for forskellighed, og fremhæver dets evne til at gøre beslutninger legitime. Han påpeger dog, at kompromiset kun gør beslutninger mere legitime og demokratiske under bestemte omstændigheder, da det ikke er alle politiske modstandere, man bør tildele legitimitet.

Dette nummer af Tidsskriftet Politik afsluttes med to boganmeldelser, hvor Jes Fabricius Møller anmelder Mogens Hermann Hansens *Hvad er en stat?*, mens Mogens Hermann Hansen anmelder Ole Thyssens *Statslegender – Filosoffernes blik på staten – fra flodstat til velfærdsstat*.